# Department of Homeland Security Daily Open Source Infrastructure Report for 07 March 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

## Daily Highlights

- The San Antonio Express−News reports federal authorities in San Antonio believe more than 250 people were victims of a debit−card scam at automated teller machines using 254 counterfeit cards made through a scam known as skimming. (See item 9)
- Perdue University has officially opened a research center to develop tools for analyzing information that could warn officials of a terrorist attack, as well as assist emergency responders. (See item 29)



# Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 06, Associated Press* — **Smokestack at West Virginia power plant catches fire.** A fire broke out Saturday, March 4, in a 1,000−foot−tall smokestack under construction at a coal−fired American Electric Power (AEP) power plant in West Virginia, briefly trapping three workers. A fourth was presumed dead, officials said. On Sunday, crews used a helicopter to inspect the smokestack. According to AEP, Sunday's helicopter inspections confirmed that the stack liner had been destroyed and that the structure on top of the stack had been partially damaged. A complete review of the inspection tapes likely will take a few days, AEP said. "Large amounts of debris are lying in the base of the stack," the company said. The men were

installing a fiberglass lining inside the concrete stack when the fire started Saturday evening at AEP's Kammer−Mitchell plant. The cause of the fire has not been determined, American Electric Power spokesperson Carmen Prati−Miller said. AEP is upgrading the coal−fired power plant to bring it into compliance with federal air pollution regulations. The plant is south of Moundsville and about 68 miles southwest of Pittsburgh, PA.
Source: http://kutv.com/topstories/local_story_065110358.html

2. *March 05, Agence France−Press* — **Spanish test olives as energy source.** More than 300 buildings in Madrid now run on energy extracted from olive cores, raising hopes that olives will become an alternative source of cheap power. "The quality of the heating is higher and more constant than natural gas or carbon, it's less dirty and less ugly than coal, the costs are lower and it is a national product which does not leave us dependent on fuel (price) fluctuations," says Jorge Tudel, chairman of the flat−owners association. But energy from the crop remains "insignificant" in the country compared with natural gas, fuel or coal.
Source: http://news.yahoo.com/s/afp/20060305/lf_afp/afplifestylespai n_060305210406

3. *March 05, Bloomberg* — **Nigerian militants vow to cut oil production by one million barrels per day.** Nigerian militants who are holding three foreign oil workers hostage said they aim to cut the West African nation's oil production by another one million barrels a day this month by increasing attacks. The attacks last month on a pipeline and the Forcados export terminal forced Royal Dutch Shell to halt output of 455,000 barrels a day, about a fifth of Nigeria's daily production. The Movement for the Emancipation of the Niger Delta (MEND) failed to carry out its threat of a 30 percent shutdown in February. The new target is excluding what has been cut off the market so far. Nigeria produced 2.36 million barrels of oil a day in January, making it the sixth−biggest producer in the Organization of the Petroleum Exporting Nations. Nigerian Oil Minister Edmund Daukoru said that the oil industry could restore three−quarters of lost production within two weeks of the hostages' release. MEND says it's planning to deliver "one huge crippling blow" to the oil industry and will expand its attacks beyond the western delta. Shell last month shut down its EA offshore oil field and all production from the western Niger delta. The Shell venture pumps about half of Nigeria's total oil production.
Source: http://www.bloomberg.com/apps/news?pid=10000085&sid=axOgPcRf 3itM

4. *March 04, New York Times* — **Consolidated Edison finds 1,214 stray voltage sites in one year.** Consolidated Edison (Con Ed) found 1,214 instances of stray voltage during a yearlong examination of electrical equipment on city streets. The stray voltage was detected from December 2004 through November 2005 on 1,083 streetlights, 99 utility poles and 32 power−distribution structures like manholes, service boxes and transformer vaults, according to test results submitted to the state's Public Service Commission, which regulates utilities. In total, 728,789 pieces of equipment were tested. John F. Miksad of Con Ed, said the company expected to spend $100 million this year toward reducing the risk of stray voltage. Despite those efforts, a series of recent mishaps have highlighted the risks of stray voltage in the city. By April, the utility will acquire five vehicle−mounted stray−voltage detection machines linked to video cameras. The machines will reduce the time it takes Con Ed to survey Manhattan for stray voltage after a snowstorm. Con Ed has assigned identification numbers, bar codes and satellite coordinates to all 172,000 poles holding streetlights and traffic signals. The company has switched to using dual−jacket rubber cables. Con Ed and the city are installing 5,000

isolation transformers, devices that prevent current from flowing through a streetlight if the wiring to the light fails.
Source: http://www.nytimes.com/2006/03/04/nyregion/04voltage.html?_r =1&oref=slogin

5. *March 03, Reuters* — **U.S. says CO2 injection could quadruple oil reserves.** The United States, where oil production has been declining since the 1970s, has the potential to boost its oil reserves four−fold through advanced injection of carbon dioxide into depleted oilfields, the Department of Energy (DOE) said. The U.S., the world's top oil consumer, has been successfully pumping small amounts or carbon dioxide into depleted oil and natural gas fields for 30 years to push out hard−to−reach fossil fuels. The DOE said 89 billion barrels could potentially be added to current proved U.S. oil reserves of 21.9 billion barrels through injection of carbon dioxide, the main gas that most scientists believe is warming the earth. The DOE gave no time frame for when the extra barrels could be added. The amount is about what the United States, at current demand, uses in 12 years. Up to 430 billion barrels could be added by pumping the gas into fields that have yet to be discovered, the DOE said.
Report: http://www.fossil.energy.gov/programs/oilgas/eor/Undeveloped_Domestic_Oil_Resources_Provi.html
Source: http://news.yahoo.com/s/nm/20060304/sc_nm/energy_crude_injec tion_dc_1

6. *March 02, Wichita Eagle (KS)* — **Oil from Canada begins flowing at Oklahoma terminal.** Canadian oil from northern Alberta began flowing to Oklahoma on Thursday, March 2. The Spearhead Pipeline was commissioned at the Cushing, OK crude oil terminal. Canada is the largest supplier of crude oil to U.S. markets at 1.6 million barrels per day. The oil sands of western Canada contain 175 billion barrels of oil reserves, second only to Saudi Arabia. The Spearhead Pipeline will enable U.S. refineries to receive greater supplies of Canadian crude at lower prices.
Source: http://www.kansas.com/mld/kansas/14000390.htm

[Return to top]

## Chemical Industry and Hazardous Materials Sector

7. *March 06, Associated Press* — **Chemical leak kills two men.** Two employees of Texas Molecular LLC in Corpus Christi, TX, a hazardous materials disposal facility, died Saturday, March 4, after inhaling fumes from a chemical leak, police said. Authorities are working to determine what chemical caused the deaths. The privately owned facility handles numerous hazardous materials from refineries, making it difficult to immediately identify the spilled chemical.
Source: http://www.wfaa.com/sharedcontent/dws/news/texassouthwest/stories/DN−spill_06tex.ART.State.Edition1.91697bf.html

[Return to top]

## Defense Industrial Base Sector

8.

*March 03, Air Force Link* — **Air Force seeks new tanker.** The Air Force wants a new refueler aircraft, something commercially available now, which can be modified to replace the existing KC−135 Stratotanker fleet. That testimony came from Air Force leaders associated with the tanker replacement program, February 28, in front of the House Armed Services Committee subcommittee on projection forces. Lt. Gen. Donald Hoffman, the military deputy for Air Force acquisition, told congressional members that his first choice would be to replace the service's fleet of aging KC−135s with a new airplane. "It should be a new aircraft, a commercial derivative, and I think we ought to buy one kind," he said. "The first 100 (should) all look the same." General Hoffman told congressional members his second choice for recapitalizing the tanker fleet would be to modernize the current KC−135 fleet, which involves converting existing KC−135E models to KC−135R models.
Source: http://www.af.mil/news/story.asp?id=123016862

[Return to top]

## Banking and Finance Sector

9. *March 05, San Antonio Express−News (TX)* — **Cloned−card scams target bank accounts in Texas.** Federal authorities in San Antonio, TX, believe more than 250 people were victims of a debit−card scam involving a pair of Houston residents. The pair was indicted in connection with about $85,000 that was withdrawn in just a few hours at automated teller machines in San Antonio using 254 counterfeit cards made through a scam known as skimming. It is not yet known how widespread the scam was. A federal grand jury in San Antonio on Wednesday, March 1, indicted Shadi Ismail Mohamed Banihani and Samer Mohamed Al−Khatib on charges of conspiring to possess and use unauthorized ATM cards. The pair were arrested Thursday, February 9. Troopers found $85,000 and 254 counterfeit ATM cards in the men's car, along with a costume mask and numerous ATM withdrawal receipts, court records show. Law officers believe Banihani captured customers' information using a skimming machine at the Houston gas station where he worked. And, officials contend, he may have obtained the PIN numbers by watching as customers keyed them in, or after the patrons carelessly released the information.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA030506.09B.atm_theft.27d5322.html

10. *March 05, Daily Herald (TN)* — **Area banks act fast to nip Visa scam.** Customers from most banks in Columbia, TN, have been at risk from a security breach at a national retailer which compromised thousands of accounts, but banks have moved quickly to halt any activity on the card numbers of potentially vulnerable accounts. Only debit card numbers, not credit cards, were affected. Mike Saporito of Community First Bank said Visa has declined to inform the bank of the retailer that experienced the data breach. Bill Fanning had $9,000 stolen from his business account and charges were made from South Africa. Paula Zimmer found that on February 26 her account had been drained via withdrawals from New Zealand, Bulgaria, and Quebec. Of the 300 Community First customers who showed up on risk alert only a few were affected. Other banks throughout Columbia also moved quickly to minimize damage. First Farmers & Merchants Bank has about 1,000 Visa debit cardholders. How the perpetrators were able to access the account numbers has still not been explained. Visa said the numbers were stolen between January 2004 and January 2005, but the fraudulent charges have only just begun

to appear on people's bank statements.
Source: http://www.columbiadailyherald.com/articles/2006/03/05/top_s tories/04visa.txt

11. *March 04, Associated Press* — **Southern California man charged for stealing IDs.** A man has been charged with skimming the electronic data from credit and debit cards and then using the numbers to take cash out of an ATM at a Northern California casino. Claudiu Hotea was indicted Thursday, March 2, in federal court in Sacramento on one count of access−device fraud. The indictment stemmed from a joint investigation by the Placer County Sheriff's Department and U.S. Secret Service into an identity theft ring involving more than 90 victims who used gas stations in Yuba, Sutter, and other counties. Investigators have said Hotea and an associate attached an illegal scanning device and mounted tiny cameras to gas pumps at service stations from Sacramento to Redding, then used the data to steal at least $110,000 from ATMs. The faceplates were attached to debit card readers to capture card data, and the cameras recorded users typing in their PIN numbers.
Source: http://sacunion.com/pages/sacramento/articles/7905

12. *March 03, Times News Network (India)* — **Pact to tackle cyber crime.** India and the U.S. on Thursday, March 2, agreed to enhance cooperation between law enforcement agencies of the two countries in tackling cyber crime. The Indian Computer Emergency Response Team and the United States National Cyber Security Division would now share expertise to trace computer viruses, software worms, and network traffic analysis. In 2001, the two countries had set up an India−US cyber security forum as part of a counter−terrorism dialogue. A joint U.S.−India statement released after talks between President George Bush and PM Manmohan Singh stressed that in view of the importance of cyber security and cyber forensic research, the two countries are also carrying out discussions on a draft protocol on cyber security.
Source: http://timesofindia.indiatimes.com/articleshow/1436207.cms

[Return to top]

## Transportation and Border Security Sector

13. *March 06, USA TODAY* — **Airline service grows in New Orleans.** U.S. airlines are rapidly adding flights at New Orleans, and the storm−ravaged city will soon have more than half the volume of its pre−Katrina air service. The number of airline seats scheduled to leave New Orleans' Louis Armstrong airport this month represents 46 percent of the year−ago total, according to schedule data from Back Aviation Solutions. For June, airlines have scheduled 57 percent of the number of departing seats in June 2005. By June, airlines will have restored non−stop flights to 33 airports, versus 44 airports before Katrina. Louis Armstrong lost all commercial air service after the August 29 hurricane. Its facilities were used to treat survivors of the storm and subsequent flooding.
Source: http://www.usatoday.com/travel/flights/2006−03−05−new−orlean s−air−usat_x.htm

14. *March 06, Toronto Star (Canada)* — **Freight train accidents soar.** Canadian freight trains are running off the rails in near record numbers and spilling toxic fluids at an alarming rate, but only a tiny fraction of the accidents is ever investigated, a Toronto Star probe shows. The number of accidents has risen each year since 2002, according to a decade's worth of accident

reports filed by the Transportation Safety Board (TSB). Last year, there were 1,246 accidents −− the most since 1996 −− and 215 of them involved toxic and dangerous materials. Freight trains are essentially mobile warehouses, traveling across the country past hundreds of thousands of backyards. Poor maintenance, human error, an over−reliance on technology and staff cuts at the two national railroads are contributing factors for the most serious accidents reviewed by the TSB. In addition, the rising accident rate comes at a time of record profits in the industry, reaping the financial benefits of 1990s layoffs, when one−third of the rail labor force was chopped.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1141599010760&call_pageid=968350130169&col=969483202845

15. *March 06, First Coast News (FL)* — **Mayday hoax calls continue, Coast Guard looking for source.** Three distress calls for help has the Coast Guard believing it has a hoax caller on its hands. Thursday, March 2's call had the Coast Guard and the Navy involved in a search off the coast of Saint Augustine, FL. Hours of work costing taxpayers more than fifty thousand dollars turned up nothing. Donnie Brzuska with Coast Guard Mayport says, "Just about every single time he called he said, 'Coast Guard, Coast Guard, Mayday, Mayday. We are going down.'" The law calls for stiff punishment of such call, and if convicted, up to ten years in jail and a $250,000 fine is possible.
Source: http://www.firstcoastnews.com/news/topstories/news−article.a spx?storyid=53170

16. *March 06, Department of Transportation* — **Mississippi receives additional money for bridges, ferry service, and road repairs.** Mississippi will get $248 million in additional federal transportation funds to rebuild hurricane−damaged highways, Department of Transportation Secretary Norman Y. Mineta announced on Monday, March 6. The federal funds will pay for new U.S. 90 bridges over Biloxi Bay and St. Louis Bay, which were wiped out by Hurricane Katrina, and provide ferry service while the bridges are under construction. The funds will also cover rebuilding U.S. 90 along the Mississippi coast and the cost of clearing debris from highways immediately after the storm. The Department of Transportation provided $25 million last year, raising the total Mississippi has received in the aftermath of Katrina to more than $1 billion to repair or rebuild federally supported highways and bridges.
Source: http://www.dot.gov/affairs/dot2206.htm

17. *March 06, Wall Street Journal* — **Smaller business jets ready, technology lags.** The use of private business jets will triple over the next decade, driven by the introduction of relatively inexpensive "microjets," the Federal Aviation Administration (FAA) predicts. The arrival of these very light jets could make corporate planes affordable to more companies and air−taxi services at smaller airports more viable financially. The new jets could pose financial challenges for commercial airlines, which are suffering financially. Already, business jets tend to siphon away first−class passengers and those who buy full−fare tickets at the last minute. The coming of very light jets also poses potential problems for air−traffic control. FAA officials worry about congestion on some runways and in the skies, where more planes may be crowding the same airspace. While these planes are small, they can fly at high altitudes alongside commercial carriers. And they require the same amount of attention from air traffic controllers as do larger aircraft, particularly if they fly through congested air space. To handle the demand from small planes −− coupled with rising demand from the commercial carriers,

expected to carry one billion passengers by 2015 −− the FAA says it must upgrade technology to allow more planes to move through the air at once.
Source: http://www.indystar.com/apps/pbcs.dll/article?AID=/20060305/BUSINESS/603050375/1003

18. *March 06, Inside Bay Area (CA)* — **Port of Oakland gets extra security.** The giant cranes hovering along the city's shoreline at the Port of Oakland soon will accomplish more than just the unloading of ships. They will help protect against a terrorist strike. With help from a $2.4 million federal grant, by 2008 the port will outfit the cranes with 60 video cameras to monitor activity on the water in front of its maritime terminals. It will be the first time in port history that its docks will be under surveillance 24 hours a day and the cameras will allow the port to meet regulations in the federal Maritime Transportation Security Act that require such monitoring. "This will add another layer of security," said Mike O'Brien, the port's facilities security officer. "This system will give us the potential for 24 hour monitoring capabilities of any activity that occurs water side."
Source: http://www.insidebayarea.com/localnews/ci_3573936

[Return to top]

## Postal and Shipping Sector

19. *March 02, News−Reporter (GA)* — **Saturday’s drill simulated anthrax at Georgia post office.** A large emergency preparedness drill was held for Wilkes County on Saturday morning, March 4, involving county health, law enforcement, medical, media, and state health agencies. The emergency exercise simulated a scenario in which anthrax has been discovered in the Athens, GA, post office, and may have spread to the mail in Wilkes County. This imaginary emergency tested the ability of local agencies including the Wilkes County Health Department, the county Emergency Management Agency, Wills Memorial Hospital, Wilkes Emergency Medical Service, and others, to respond to the threat. Volunteers played the part of patients during the exercise, which took place at WashingtonWilkes Comprehensive High School. Saturday’s exercise was a hands−on training that simulated the treatment of large numbers of citizens in a controlled environment, using the actual agencies and personnel who would be involved in a real emergency in Wilkes County.
Source: http://www.news−reporter.com/news/2006/0302/Front_Page/002.h tml

[Return to top]

## Agriculture Sector

20. *March 06, Agricultural Research Service* — **Africanized honeybees are still on the move.** In 2005, Africanized honeybees showed up for the first time in Louisiana, Arkansas, and Florida. The arrival in Florida was not contiguous with the bees' spread from the Southwest. It was most likely a result of human−assisted transport, by which trucks, ships, railroad cars, or other types of transportation inadvertently bring Africanized honeybees into new areas. Usually, human−assisted transport finds are not considered part of Africanized honeybees' spread. But because they have been found in 14 counties, the state of Florida now considers Africanized

honeybees to be established there. Among Agricultural Research Service's recent research accomplishments related to the bees is new guidance for beekeepers on the best time to requeen hives to reverse Africanization of honeybee colonies. Queens of known genetics, from reputable breeders, should be introduced into hives in the fall to give them the best chance of being accepted by the bee colony.
Map showing the spread of Africanized honeybees: www.ars.usda.gov/ahbmap/
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

**21.** *March 03, North Dakota Ag Connection* — **North Dakota joins security consortium.** North Dakota is now part of a 12−state cooperative effort to deal with naturally occurring and artificially induced biological threats to agriculture. Agriculture Commissioner Roger Johnson and State Veterinarian Susan Keller have signed the agreement by which the North Dakota Department of Agriculture (NDDA) and the State Board of Animal Health (BOAH) joined the Multi−State Partnership for Security in Agriculture. Johnson said the partnership has focused efforts on the following priorities: development of plant and animal disease risk communication materials, development of model agricultural emergency response plans, and review and evaluation of state training programs and exercises. The partnership is also developing cross−border training and exercise scenarios recognizing that disease outbreaks or other events affecting agriculture will not stop at state borders. Formed in August 2003, the partnership is comprised of the agriculture departments, state veterinarian's offices, homeland security advisors, animal health departments, and emergency management divisions in North Dakota, Illinois, Iowa, Kansas, Kentucky, Minnesota, Missouri, Nebraska, Ohio, Oklahoma, South Dakota, and Wisconsin.
Source: http://www.northdakotaagconnection.com/story−state.cfm?Id=16 1&yr=2006

**22.** *March 01, Purdue University* — **Center for crop biosecurity.** Purdue University has created a center that could be vital in the national effort to protect the country's food supply against foreign plant pests and pathogens that might be introduced through natural means or terrorism. The existing Purdue University Plant & Pest Diagnostic Laboratory, which is part of the new center, already is part of the National Plant Diagnostic Network. In addition, Purdue, along with various research organizations and the federal government have discussions under way about establishing a national plant biosecurity center within the U.S. Department of Agriculture. The purpose of Purdue's new center is to identify plants and pathogens that could cause damage to U.S. crops, to find pathways through which pathogens could invade, and to determine how to prevent their introduction. Experts at Purdue's center will provide education to those who must be on the front lines in dealing with invasions by harmful pests and pathogens.
Source: http://news.uns.purdue.edu/UNS/html4ever/2006/060301.Martyn. biosecurity.html

[Return to top]

## Food Sector

**23.** *March 03, Canadian Food Inspection Agency* — **Canadian Food Inspection Agency completes bovine spongiform encephalopathy investigation.** The Canadian Food Inspection Agency (CFIA) has concluded its investigation into the case of bovine spongiform encephalopathy (BSE) confirmed on January 22, 2006. No additional cases of the disease were detected during the investigation. The investigation traced two of the affected animal’s

offspring and 156 cattle born on the farm of origin within 12 months before and after the affected animal's birth. The CFIA considered several potential sources of infection, of which contaminated feed was the most probable. Investigators examined what the affected animal may have consumed early in its life when cattle are most susceptible to the BSE agent. Although a definitive origin could not be confirmed, the CFIA believes that the animal's feed was likely contaminated during its manufacture, transport, or storage.
Investigation summary: http://www.inspection.gc.ca/english/anima/heasan/disemala/bseesb/ab2006/4investe.shtml
Source: http://www.inspection.gc.ca/english/corpaffr/newcom/2006/200 60303e.shtml

[Return to top]

## Water Sector

Nothing to report.
[Return to top]

## Public Health Sector

**24.** *March 06, Associated Press* — **Austrian cats test positive for bird flu.** Several cats have tested positive for the H5N1 strain of bird flu in Austria's first reported case of the disease spreading to an animal other than a bird, state authorities said Monday, March 6. Two or three cats, all of which are still alive, have tested positive for the H5N1 strain of the disease, Hans Seitinger, the top agriculture official in the southern state of Styria, told state broadcaster ORF. German authorities last month confirmed that a cat on the Baltic Sea island of Ruegen had succumbed to the deadly virus, which it is believed to have caught by eating an infected bird. That would be consistent with a pattern of disease transmission seen in wild cats in Asia. According to the World Health Organization, several tigers and snow leopards in a zoo and several house cats were infected with H5N1 during outbreaks in Asia in 2003 and 2004.
Source: http://www.breitbart.com/news/2006/03/06/D8G64A380.html

**25.** *March 06, Agence France−Presse* — **Experts draw up pandemic flu battle plan at World Health Organization.** Experts began meeting at the World Health Organization (WHO) to refine plans for rapid detection and containment of a potential global flu pandemic, amid concern about the spread of highly pathogenic H5N1 avian influenza in birds. The technical meeting is due to work on a "protocol for rapid containment and response", to ease the detection of the first signs of a new, more deadly and infectious strain of flu in humans that could spread swiftly around the world. The original draft of the plan, one of a series to coordinate international action, was first released in January. But the outcome of the latest three−day discussion is not expected to be available until March 15, WHO spokesperson Dick Thompson said. One of the key challenges for experts is how to define the early warning signs of a pandemic strain of influenza. Other factors for concern could include clusters in several locations, the presence of H5N1 or concurrent seasonal influenza.
WHO Avian Influenza Rapid response and containment draft protocol:
http://www.who.int/csr/disease/avian_influenza/guidelines/Ra pidResponse_27%2001.pdf
Source: http://news.yahoo.com/s/afp/20060306/hl_afp/healthfluwhoplan

_060306140935;_ylt=AqyofTpZStS9B5PkoNW.atKJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**26.** *March 05, Agence France−Presse* — **China sees ninth bird flu death.** China confirmed that a ninth person had died from bird flu, state media reported, while Azerbaijan said it was checking if two children may have died from the illness. As the spread of the disease continued −− with France, Germany, Greece, Poland, Romania, and Switzerland all announcing new confirmed or suspected cases in birds −− authorities in Europe, Asia, and Africa stepped up measures to prevent a pandemic. Hong Kong, which borders the province of Guangdong where the latest Chinese fatality occurred, slapped a ban on imports of poultry and other birds from Guangdong. Poland and France imposed hygiene safety defenses around new infected areas and Nigeria promised neighboring Niger equipment and training to stem the virus' advance. China's health ministry said a 32−year−old man who had frequented poultry markets had succumbed to bird flu in Guangdong. Azerbaijan said it was checking samples from two children who died in the Asian part of the country. If confirmed, Azerbaijan would be the second country that straddles Europe and Asia to have human victims. Tests were also being conducted on four of their relatives, who are in hospital.
Source: http://news.yahoo.com/s/afp/20060305/wl_asia_afp/healthfluworld_060305192256;_ylt=AuY__ivLl.DW8AAI8Nm1.3.JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**27.** *March 02, Press Trust of India* — **Fever affects 3,000 people in Rourkela.** Despite efforts to control it, an air−borne fever has affected around 3, 000 people in Rourkela, India, and the disease is slowly taking epidemic form. The viral fever was spreading unexpectedly and the number of people affected had risen up to 3,000 till March 1 Chief District Medical Officer, Premananda Patnaik said. The fever has also been reported from Kishantola, Chhend Colony, Rukutola, Railway Colony, PHD Colony and Banglatoli, most of them located in slums.
Source: http://www.ibnlive.com/article.php?id=6203&section_id=3

[Return to top]

## Government Sector

**28.** *March 06, Associated Press* — **Powder causes scare at Georgia state office building.** At least five people in a Georgia state office building were decontaminated by rescue officials Monday, March 6, after a white powdery substance was detected in an envelope and two employees complained of a reaction to it. It wasn't immediately clear what the substance was. It was discovered by an employee in a Department of Corrections mailroom across the street from Georgia's Capitol, said Ken Davis, spokesperson for the Georgia Office of Homeland Security.
Source: http://www.boston.com/news/nation/articles/2006/03/06/powder_causes_scare_ga_office_building/

[Return to top]

## Emergency Services Sector

29. *March 06, Perdue University (IL)* — **Purdue opens center to analyze homeland security data.** Purdue University opens a research center to develop tools for analyzing information that could warn officials of a terrorist attack, and assist emergency responders. A kick−off event will take place for the Purdue University Regional Visualization and Analytics Center Tuesday, March 7. Jim Thomas, director of the Department of Homeland Security National Visualization and Analytics Center, and Eric Dietz, executive director of the Indiana Department of Homeland Security, will explain how the center will develop technology to improve national security. Thomas said the center will equip a team of Purdue and Indiana University School of Medicine researchers to create tools to analyze vast amounts of information involving intelligence analysis, emergency planning and health−care monitoring. The team's tools will then be deployed for use by homeland security and emergency response personnel.
Source: http://news.uns.purdue.edu/hp/Ebert.Purvac.html

30. *March 04, Associated Press* — **Mississippi officials to unveil prototype of emergency text messaging system.** Mississippi Homeland Security officials this month will unveil a prototype of an emergency text messaging system that would provide reliable communications to first responders during catastrophes like Hurricane Katrina. The system would make it possible for text messages to be sent over Mississippi Public Broadcasting's FM radio signals to first responders. Mississippi would be the first state with such an emergency communication system, officials said.
Source: http://www.picayuneitem.com/articles/2006/03/04/news/12text. txt

31. *March 04, Associated Press* — **Controversy over historic fire alarms in Pennsylvania.** Pittsburgh got rid of them decades ago, and Erie city workers are tearing them off utility poles this month because the city is merging its police and fire dispatch centers. But firefighters in other cities say Gamewell master boxes −− those little red fire alarms that have summoned emergency crews to city streets across the country and overseas with one pull of a white lever for more than 150 years −− are still useful, despite the availability of newer technology. Critics say cell phones and emergency radios rendered the alarms obsolete. Proponents say simplicity is what makes the Gamewells so valuable. The boxes send a simple alarm signal over underground telegraph wires pinpointing the box's location. The boxes use a spring loaded crank to send the electrical alarm impulses over the wire, and work even when electricity is out because they have a self−contained power supply.
Source: http://www.newsday.com/news/local/wire/connecticut/ny−bc−ct−−alarmboxes0304mar04,0,3441380.story?coll=ny−region−apconnec ticut

32. *March 03, Journal & Topics (IL)* — **Illinois city receives new rapid intervention vehicle.** A new emergency vehicle designed specifically for airline crashes is now operable in Prospect Heights, IL. The rapid intervention vehicle carries 1,000 gallons of water, 130 gallons of foam, 500 pounds of fire extinguishing powder, and huge tires to handle off−road conditions at a crash site. One unique feature of the vehicle is its ability to shoot water while the truck is moving. In addition, the fire extinguishing agent can surround a burning substance and is particularly effective in surrounding fuel, which would otherwise continue to reignite.
Source: http://www.journal−topics.com/ph/06/ph060303.1.html

[Return to top]

# Information Technology and Telecommunications Sector

**33.** *March 06, Sydney Morning Herald (Australia)* — **New safety net for Web surfers.** A fresh approach to "safe surfing" has been dreamt up by a group of Massachusetts Institute of Technology engineers involved in a crusade to make the Internet a safer place for their friends and families. The result of their labors is a product called SiteAdvisor which labels particular Websites with a color−coded security rating to help users identify those that might contain spyware, spam, viruses, and online scams. The millions of Websites on the Internet are trawled using sophisticated computer "robots" that can intelligently analyze the safety of a given destination. The tool then presents its findings alongside search engines such as Google, Yahoo! or MSN and labels results as either green, yellow or red.
SiteAdvisor: http://www.siteadvisor.com/preview/
Source: http://www.smh.com.au/news/breaking/new−safety−net−for−web−surfers/2006/03/06/1141493583941.html

**34.** *March 06, IDG News Service* — **AT&T to buy BellSouth in $67 billion deal.** AT&T on Sunday, March 5, announced a deal to acquire U.S. telecommunications operator BellSouth Corp. in an all−stock deal valued at $67 billion. The merger will mean faster development of Internet Protocol TV (IPTV) services for U.S. consumers, drawing on AT&T's research and development work on IPTV and BellSouth's existing fiber−optic networks for DSL and other broadband services, AT&T said.
Source: http://www.infoworld.com/article/06/03/06/76115_HNattbuybell south_1.html

**35.** *March 05, FrSIRT* — **IBM WebSphere Application Server Java SDK multiple vulnerabilities.** Multiple vulnerabilities have been identified in IBM WebSphere Application Server, which could be exploited by remote attackers or malicious Websites to compromise a vulnerable system. Analysis: These flaws are due to errors in Java "reflection" APIs. Affected products: IBM WebSphere Application Server version 5.x and IBM WebSphere Application Server version 6.x.
Solution: Apply fixes: http://www−1.ibm.com/support/docview.wss?uid=swg27004980
Source: http://www.frsirt.com/english/advisories/2006/0828

**36.** *March 04, Security Focus* — **Microsoft IIS authentication method disclosure vulnerability.** Microsoft IIS supports Basic and NTLM authentication. Reportedly, the authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted. Analysis: When a valid authentication request is submitted for either message with an invalid username and password, an error message will be returned. This happens even if anonymous access to the requested resource is allowed. An attacker may be able to use this information to launch further intelligent attacks against the server, or to launch a brute−force password attack against a known username.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/4235/info.
Solution: Currently the Security Focus staff is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/4235/references

37. *March 03, Information Week* — **Newest Bagle worm threatens legal action.** Another Bagle worm appeared Friday, March 3. Bagle.do, said UK−based Sophos, spreads in e−mails with subject lines such as "Lawsuit against you." The attached file, with names like "lawsuit.exe," purports to be supporting legal documents. Launching the executable file infects the PC with a backdoor and lowers the machine's security settings, and may end up with more malicious code downloaded to the system from a slew of Websites.
Source: http://www.informationweek.com/news/showArticle.jhtml?articleID=181500852&subSection=Columns

38. *March 03, eWeek* — **RIM, NTP settle case: BlackBerry service is safe.** BlackBerry maker Research In Motion (RIM) and patent−holding company NTP on Friday, March 3, announced that both parties have entered into a settlement agreement and a license that will end the patent litigation that had been threatening to shut down BlackBerry service in the United States. Under the terms of the settlement, RIM will make a one−time payment to NTP of $612.5 million. In return, NTP has granted RIM a license that will let RIM continue its BlackBerry−related wireless business, according to officials at both companies. The license covers all the current wireless e−mail patents involved in the litigation as well as any future NTP patents, officials said. The resolution also protects all the wireless carriers and channel partners who sell BlackBerry products, as well as any other hardware makers who have licensed BlackBerry software for use in their own devices.
Source: http://www.eweek.com/article2/0,1895,1933824,00.asp

## Internet Alert Dashboard

### DHS/US−CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing

Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#sgener al

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 80 (www), 139 (netbios−ssn), 32459 (−−−), 32774 (sometimes−rpc11), 49200 (−−−), 55551 (−−−)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

# General Sector

Nothing to report.
[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

**DHS Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.